APPARATUS AND METHOD FOR ID-BASED RING SIGNATURE BY USING BILINEAR PAIRINGS

Field of the Invention

The present invention relates to a cryptographic system based on a ring signature; and, more particularly, to a system for an identity-based ring signature by using a bilinear pairing.

Background of the Invention

In a public key cryptosystem, each user has two keys, a private key and a public key. The binding between the public key (PK) and the identity (ID) of a user is obtained via a digital certificate. However, in a certificate-based system, before using the public key of a user, the participant must first verify the certificate of the user. As a consequence, this system requires a large amount of computing time and storage when the number of users increases rapidly.

In 1984 Shamir (A. Shamir, Identity-based cryptosystems and signature schemes, Advances in Cryptology-Crypto 84, LNCS 196, pp.47-53, Springer-Verlag, 1984) suggested ID-based encryption and signature schemes to simplify key management procedures in a certificate-based

public key cryptosystem. Since then, many ID-based encryption schemes and signature schemes have been proposed.

Bilinear pairings, namely the Weil pairing and the Tate pairing of algebraic curves, are important tools for research on algebraic geometry. The early applications of the bilinear pairings in cryptography were used to evaluate a discrete logarithm problem. For example the MOV attack (using Weil pairing) and FR attack (using Tate pairing) reduce the discrete logarithm problem on some elliptic curves or hyperelliptic curves to a discrete logarithm problem in a finite field. However, the bilinear pairings have been found in various applications to cryptography recently. More precisely, they can be used to construct ID-based cryptographic schemes. Many ID-based cryptographic schemes have been proposed by using the bilinear pairings. Examples are Boneh-Franklin's ID-based encryption scheme (D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, Advances in Cryptology-Crypto 2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001.), Smart's ID-based authentication key agreement protocol (N.P. Smart, Identity-based authenticated key agreement protocol based on Weil pairing, Electron. Lett., Vol.38, No.13, pp.630-632, 2002.), and several ID-based signatures schemes, and the like.

The ID-based public key cryptosystem can be an alternative for a certificate-based public key cryptosystem, especially when efficient key management and moderate

security are required. In a public key cryptosystem, verifier's anonymity is protected by means of blind signature, whereas a signer's anonymity is protected by a ring digital signature (simply referred to as a ring signature) or a group digital signature.

The concept of ring signature was introduced by Rivest, Shamir and Tauman (R.L. Rivest, A. Shamir and Y. Tauman, How to leak a secret, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp.552-565, Springer-Verlag, 2001). A ring signature is considered to be a simplified group signature that has only users without revocation managers. It protects the anonymity of a signer since a verifier knows that the signature comes from a member of a ring, but doesn't know exactly who the signer is. There is also no way to revoke the anonymity of the signer. The ring signature can support an ad hoc subset formation and in general does not require a special setup. Rivest-Shamir-Tauman's ring signature scheme relies on a general public-key cryptosystem.

A general ring signature system requires a large amount of computing time and storage. An ID-based ring signature system using the bilinear pairings is not yet proposed, while many ID-based cryptographic schemes have been proposed by using the bilinear pairings.

Summary of the Invention

It is, therefore, an object of the present invention to provide an apparatus and a method for generating a ring signature based on identity and bilinear pairings, which not only reduces overall computing time and required storage but also simplifies key management procedures.

In accordance with one aspect of the present invention, there is provided a method for generating an identity-based ring signature by using bilinear pairings, in a cryptosystem that includes a user, a signer and a trusted authority, which includes the steps of: (a) at the trusted authority, generating a set of system parameters shared by the user and the signer and storing the set of system parameters in a memory of each of the user and the signer; (b) at the trusted authority, generating a public key and a private key for the user and the signer by using the set of system parameters, thereby transmitting the generated public and the private keys to the user and the signer through a secure channel, respectively; (c) at the user, concealing content of a message and requesting a ring signature for the content-concealed message to the signer; (d) at the signer, producing the ring signature based on identity (ID) of the user, thereby forming an ID-based ring signature for the content-concealed message; and (e) at the user, verifying validity of the ID-based ring signature.

In accordance with another aspect of the present invention, there is an apparatus for an identity-based ring signature using bilinear pairings, including: a trusted authority; a user; and a signer, wherein the apparatus performs the steps of: at the trusted authority, generating a set of system parameters shared by the user and the signer and storing the set of system parameters in a memory of each of the user and the signer; at the trusted authority, generating a public key and a private key for the user and the signer by using the set of system parameters, thereby transmitting the generated public and the private keys to the user and the signer through a secure channel, respectively; at the user, concealing content of a message and requesting a ring signature for the content-concealed message to the signer; at the signer, producing the ring signature based on identity (ID) of the user, thereby forming an ID-based ring signature for the content-concealed message; and at the user, verifying validity of the ID-based ring signature.

Brief Description of the Drawings

The above and other objects and features of the present invention will become apparent from the following description of a preferred embodiment given in conjunction with the accompanying drawings, in which:

Figs. 1A to 1C show schematic block diagrams for describing an ID-based ring signature scheme in accordance with a preferred embodiment of the present invention, respectively; and

Figs. 2A and 2B represent a flow chart for describing an ID-based ring signature procedure in accordance with a preferred embodiment of the present invention.

Detailed Description of the Preferred Embodiments

An identity (ID)-based ring digital signature scheme in accordance with the present invention may be viewed as a combination of a ring signature scheme and an ID-based signature scheme. Further, the ID-based ring signature scheme of the present invention uses bilinear pairings.

The ID-based ring signature of the present invention includes following four procedures:

1. Setup: determining system parameters PARAMS and a master key s.

2. Extract: taking the master key s and an identity (ID) of a signer; and generating a private key S_{ID} and a public key Q_{ID} of the signer.

3. Signing: taking the PARAMS, the private key of the signer, a list L and a content-concealed message m; and outputting an ID-based ring signature $\sigma(m)$ for m, wherein the list L is a set of identities of users.

4. Verification: taking the list L, the content-concealed message m and the ID-based ring signature $\sigma(m)$; and checking whether the ID-based ring signature $\sigma(m)$ is valid or not.

An apparatus and a method based on the above-mentioned ID-based ring signature scheme in accordance with the present invention will be described in detail with reference to Figs. 1A to 2B.

A signer 100, a user 200 and a trusted authority 300 act as participants of the ID-based ring signature scheme. Herein, each of the participants may be a computer system and they communicate remotely through any kind of communications network or other techniques. Information to be transferred between the participants may be stored and/or detained in various types of storage media.

Fig. 1A shows a schematic block diagram for describing Setup and Extract procedures of an ID-based ring signature system in accordance with the present invention.

The trusted authority 300 generates system parameters (PARAMS) to be utilized by the signer 100 and the user 200, and selects a master key. Further, the trusted authority 300 produces a public key and a private key of each of the signer 100 and user 200 based on identities of the signer 100 and the user 200, and thereafter, provides the keys to the signer 100 and the user 200 through secure channels. The trusted authority 300 participates in the Setup and

Extract procedures, but does not participate in subsequent procedures anymore.

Fig. 1B depicts a schematic block diagram for describing a Signing procedure of the ID-based ring signature system in accordance with the present invention.

First, the user 200 conceals content of a message and provides the content-concealed message to one of signers to request a digital signature (more specifically, an ID-based ring signature) for the message.

If the signer 100 receives the request of the signature and the content-concealed message, the signer 100 generates an ID-based ring signature for the content-concealed message without knowing the content of the content-concealed message, based on the PARAMS, by using its own private key.

Referring to Fig. 1C, the user 200 verifies whether the ID-based ring signature provided from the signer 100 is valid or not by using n+1 signature values, the content-concealed message, the PARAMS, the list L and the public key of the signer 100.

A method for the ID-based ring signature in accordance with the present invention will be described in detail with reference to a flow chart shown in Figs. 2A and 2B. In Figs. 2A and 2B, it is assumed that the number of the users participating in the ID-based ring signature scheme is "n" and a content-concealed message to be signed is transferred

or stored in a digital form.

At step 201, two cyclic groups G and v, whose orders are equal to "q", are introduced.

To be more specific, a generator P is chosen to introduce the cyclic group G and the other cyclic group V is subsequently introduced by a bilinear pairing "e", wherein the cyclic group G is an elliptic or hyper-elliptic curves Jacobian and the cyclic group V is a cyclic multiplicative group conventionally corresponding to Z_q^*. The bilinear pairing "e" from the cyclic group G to the cyclic multiplicative group V is given as follows:

$$e: G \times G \rightarrow V.$$

At step 202, cryptographic hash functions H and H_1 are determined as follows:

$$H: \{0,1\}^* \rightarrow Z_q^* \text{ and } H_1: \{0,1\}^* \rightarrow G.$$

At step 203, a random number "s" is chosen as a master key, "s" being an element of Z_q^*, and a public key P_{pub} of the trusted authority 300 is generated, by the master key s and the generator P of the cyclic group G, as follows:

$$P_{pub} = s \cdot P.$$

The public key P_{pub} of the trusted authority 300 may be established before or simultaneously with the determination of the cryptographic hash functions H and H_1.

At step 204, a set of system parameters (PARAMS) {G, q, P, P_{pub}, H, H_1} is opened and shared by the signer 100 and the user 200, to be stored in each memory thereof.

At step 205, a public and a private key of each of the signer 100 and the user 200 are produced at the trusted authority 300. If, for example, the user 200 has an identity ID_i, a public key Q_{IDi} and a private key S_{IDi} of the user 200 of ID_i are produced as follows:

$$Q_{IDi} = H_1(ID_i) \text{ and } S_{IDi} = s \cdot Q_{IDi}$$

wherein "i" is an integer from 1 to n as a user index.

The public Q_{IDi} and the private key S_{IDi} are transmitted through a secure channel and stored in a memory of the user 200 of the ID_i.

Subsequently, Signing procedure is carried out.

At step 206, the user 200 content of a message to request a signature (more exactly, ID-based ring signature) for the content-concealed message to a signer.

At step 207, after receiving the content-concealed message and the request of the ID-based ring signature for the content-concealed message from the user 200, the signer 100 takes an ID list L and extracts a random element A from the cyclic group G to thereby compute an initial signature value c_{k+1} as follows:

$$c_{k+1} = H(L \parallel m \parallel e(A, P)),$$

wherein "m" is the content-concealed message to be signed and the ID list L is a set of identities of users (i.e., $L=\{ID_i\}$).

Then the initial signature value c_{k+1} is stored in a memory of the signer 100.

At step 208, "T_i" is randomly chosen from the cyclic group G, thereby computing and storing in a memory of the signer 100 an additional signature value c_{i+1} as follows:

$$c_{i+1} = H(L \parallel m \parallel e(T_i, P)\ e(c_i\ H_1(ID_i), P_{pub})),$$

wherein "i" corresponds to k+1,···, n-1, 0, 1, k-1 (i.e., one of values of all modulo n).

At step 209, a ring signature value T_k is computed as follows:

$$T_k = A - c_k\ S_{IDk},$$

wherein S_{IDk} is a private key of the signer 100 made at step 205.

The ring signature value T_k is stored in a memory of the signer 100.

At step 210, zero is selected as a glue value (i.e., n) of the additional signature value to thereby form a ring of ring signature values and then an ID-based ring signature of n+1 ring signature values for the content-concealed message m is obtained in a following sequence (c_0, T_0, T_1,···, T_{n-1}).

Then the ID-based ring signature is forwarded to and stored in a memory of the user 200

Finally, Verification procedure is carried out.

At step 211, it is determined by the user 200 whether the ID-based ring signature is valid or not based on the following Equation

$$c_{i+1} = H(L \parallel m \parallel e(T_i, P)\ e(c_i\ H_1(ID_i), P_{pub})).$$

More specifically, a signature value sequence $\{c_i\}$ can be obtained as follows:

$$c_{k+1} = H(L \| m \| e(A, P))$$

$$c_{k+2} = H(L \| m \| e(T_{k+1}, P)\, e(c_{k+1} H_1(ID_{k+1}), P_{pub}))$$

$$\vdots \qquad\qquad \vdots$$

$$c_n = H(L \| m \| e(T_{n-1}, P)\, e(c_{n-1} H_1(ID_{n-1}), P_{pub}))$$

$$c_1 = H(L \| m \| e(T_0, P)\, e(c_0 H_1(ID_0), P_{pub}))$$

$$c_2 = H(L \| m \| e(T_1, P)\, e(c_1 H_1(ID_1), P_{pub}))$$

$$\vdots \qquad\qquad \vdots$$

$$c_k = H(L \| m \| e(T_{k-1}, P)\, e(c_{k-1} H_1(ID_{k-1}), P_{pub}))$$

wherein i= 0, 1, …, n-1.

The obtained signature value sequence $\{c_i\}$ is stored in a memory of the user 200.

Meanwhile, in the signing procedure, the initial signature value c_{k+1} can be calculated as follows:

$$\begin{aligned} & c_{k+1} \\ &= H(L \| m \| e(T_k, P)\, e(c_k H_1(ID_i), P_{pub})) \\ &= H(L \| m \| e(A - c_k S_{IDk}, P)\, e(c_k H_1(ID_i), P_{pub})) \\ &= H(L \| m \| e(A, P)\, e(-c_k S_{IDk}, P)\, e(c_k H_1(ID_i), P_{pub})) \\ &= H(L \| m \| e(A, P)\, e(-c_k H_1(ID_i) + c_k H_1(ID_i), P_{pub})) \\ &= H(L \| m \| e(A, P)) \end{aligned}$$

In order that the signature is valid, the glue value should be zero (i.e., $c_n=c_0$) since the signature value sequence $\{c_i\}$ in the Verification procedure is the same as the Signing procedure. Accordingly, if i=0, 1,⋯,n-1 and $c_n=c_0$, then the ID-based ring signature is accepted to be

valid at step 212; and if otherwise, the ID-based ring signature is rejected at step 213.

As a conclusion, the ID-based ring signature in accordance with the present invention exhibits properties as followings.

I. Correctness

The signature value sequence $\{c_i\}$ in the Verification procedure should be the same as that in the Signing procedure. Accordingly, it can be verified whether the generated ID-based ring signature is valid or not.

II. Security

The ID-based ring signature holds unconditionally signer-ambiguity, because all T_i but T_k are taken randomly from G. In fact, the T_k is also distributed uniformly over G, since A is randomly chosen from G. Therefore, $|G|^n$ solutions, all of which can be chosen by the Signing procedure with equal probability, for fixed L and m, (T_0, $T_1, \cdots, T_{n-1}$) exist regardless of a signer.

Further, the ID-based ring signature of the present invention is considered to be non-forgeable since the probability of the following c_0 is 1/q.

$$C_0 = H(L \parallel m \parallel e(T_{n-1}, P)\ e(c_{n-1} H_1(ID_{n-1}), P_{pub}))$$

III. Efficiency

The ID-based ring signature scheme in accordance with the present invention can be performed with elliptic curves or hyper-elliptic curves, and employs a bilinear pairing.

Furthermore, the length of signature can be reduced by a factor of 2 by using compression technique.

Since the ID-based ring signature is based on identity rather than an arbitrary number, a public key has some aspects of user's information, which may uniquely identify the user, such as email address. In some applications, the lengths of public keys and signatures can be also reduced because the length of signature can be reduced.

While the invention has been shown and described with respect to the preferred embodiments, it will be understood by those skilled in the art that various changes and modifications may be made without departing from the spirit and scope of the invention as defined in the following claims.